ESG Lab Review

ForeScout Extended Modules for Palo Alto Networks

Date: January 2018 **Author:** Tony Palmer, Senior Validation Analyst

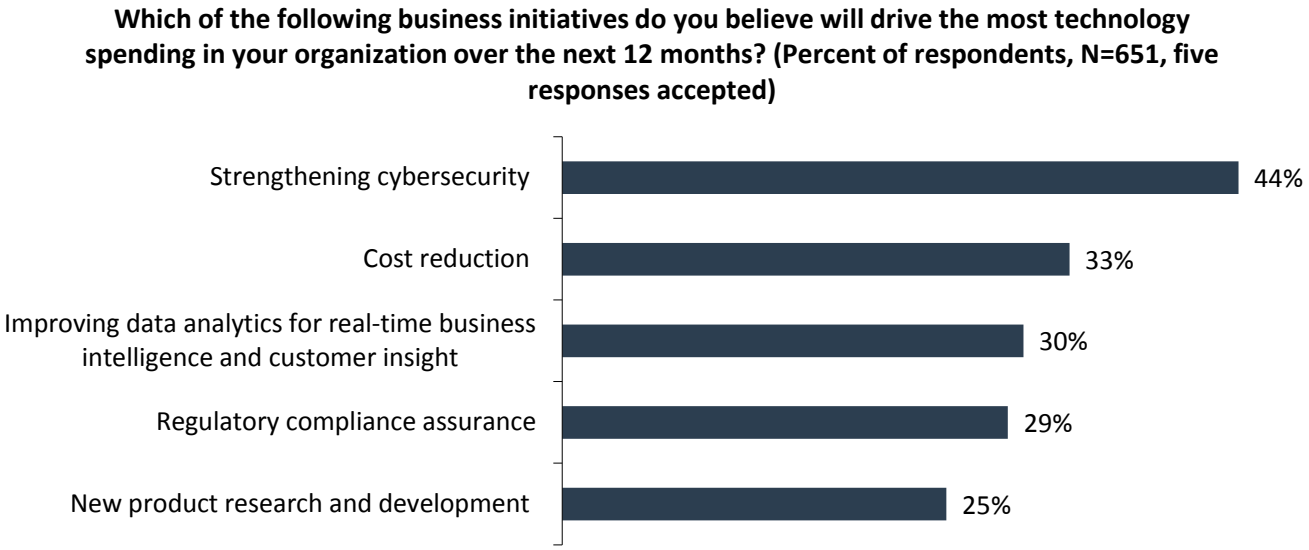
Abstract

This report provides a first look at the key benefits of ForeScout CounterACT's integration with Palo Alto Networks next-generation firewall (NGFW) and Palo Alto Networks WildFire threat analysis service. ESG Lab focused on how the ForeScout Extended Modules can combine ForeScout's endpoint insight, classification, and control capabilities with Palo Alto Networks' NGFW traffic classification, fine-grained security policies, and WildFire multilayered, cloud-delivered, advanced threat analysis security service. This integration is designed to provide more than just visibility into and classification of users and devices; it shares endpoint properties and labels to enhance dynamic segmentation, provides real-time user identity and context information in support of Palo Alto Networks' fine-grained security policies and enforcements, and detects known and unknown advanced threats and prevents them from laterally spreading.

The Challenges

According to ESG research, strengthening cybersecurity was cited by 44% of respondents as the business initiative that would drive the most technology spending in 2018 (see Figure 1).[1]

Figure 1. Top Five Business Initiatives Driving IT Spending in 2018



Source: Enterprise Strategy Group, 2018

This is hardly surprising, considering the multitude of cybersecurity incidents organizations are experiencing. In a research project conducted by ESG and the Information Systems Security Association (ISSA), 39% of cybersecurity professionals said that their organization had experienced one or more incidents resulting in the need to reimage one or more endpoint or server, 27% reported experiencing a ransomware incident, and 20% stated they had experienced at least one security incident that disrupted a business application.[2] Adding to these challenges is an increasing skills gap in cybersecurity. Fifty-one percent of organizations claim that they have a problematic shortage of cybersecurity skills—the most frequently cited

[1] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

[2] Source: ESG/ISSA Research Report, *Through the Eyes of Cyber Security Professionals: Annual Research Report (Part II)*, December 2016.

response by a wide margin.[3] The increase in mobile, personal, transient, and even virtual devices leaves many organizations unaware of a significant percentage of the endpoints on their networks. These devices are either not under management, have nonfunctional agents, or are only detected during intermittent scans.

The ForeScout Extended Modules for Palo Alto Networks

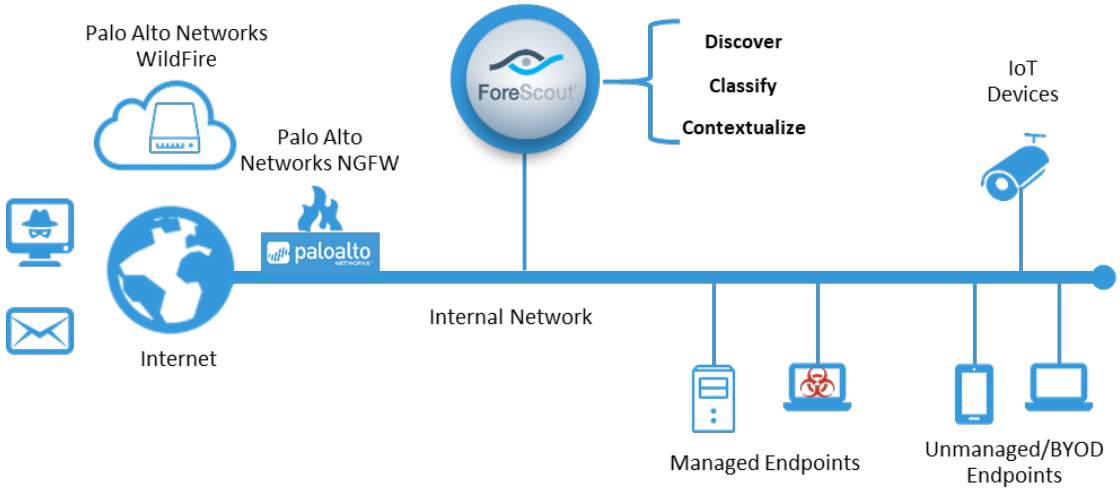
The ForeScout CounterACT platform is designed to provide continuous security monitoring and remediation for an organization's devices, both traditional and nontraditional, when they connect to the network. ForeScout's goal is to provide IT organizations with comprehensive insight into their endpoint landscape and compliance, and to address network access and threat management challenges.

In conjunction with ForeScout CounterACT, the ForeScout Extended Module for Palo Alto Networks NGFW provides visibility, classification, and exchange of real-time user and device contextual information. The ForeScout Extended Module for Palo Alto Networks WildFire uses indicator of compromise (IOC) details identified by WildFire—for example, file size, files created or modified, Windows registry changes, or processes spawned. CounterACT can isolate the infected endpoint and initiate appropriate remediation actions, then scan other endpoints on the network, including those attempting to connect, for the new IOC, and initiate threat-mitigation actions on infected endpoints.

These integrations provide visibility and control of endpoints on the network, enabling dynamic segmentation of network resources to provide approriate resource access regardless of location. In addition, organizations can enforce identity and context-aware security policies to reduce their attack surface, limit data breaches, and detect and contain advanced threats.

Cyber-attacks rely on stealth and persistence to bypass traditional security defenses. Once inside, attackers can move laterally across organizations' networks to gain access to important applications and sensitive information. Unmanaged, bring-your-own-device (BYOD), guest, and Internet of Things (IoT) endpoints are often unpatched, lack security agents, and include unauthorized applications. Hence, they can serve as network-attached launching points for threats. The combination of ForeScout's endpoint visibility, access control, and automated response capabilities with Palo Alto Networks NGFW provides real-time visibility and precise, automated controls for secure access to critical applications and resources.

Figure 2. ForeScout Extended Module for Palo Alto Networks NGFW



The joint solution enables IT organizations to implement dynamic network segmentation, create context-aware security policies within Palo Alto Networks NGFWs based on endpoint context from CounterACT, and achieve integrated threat detection and response automation.

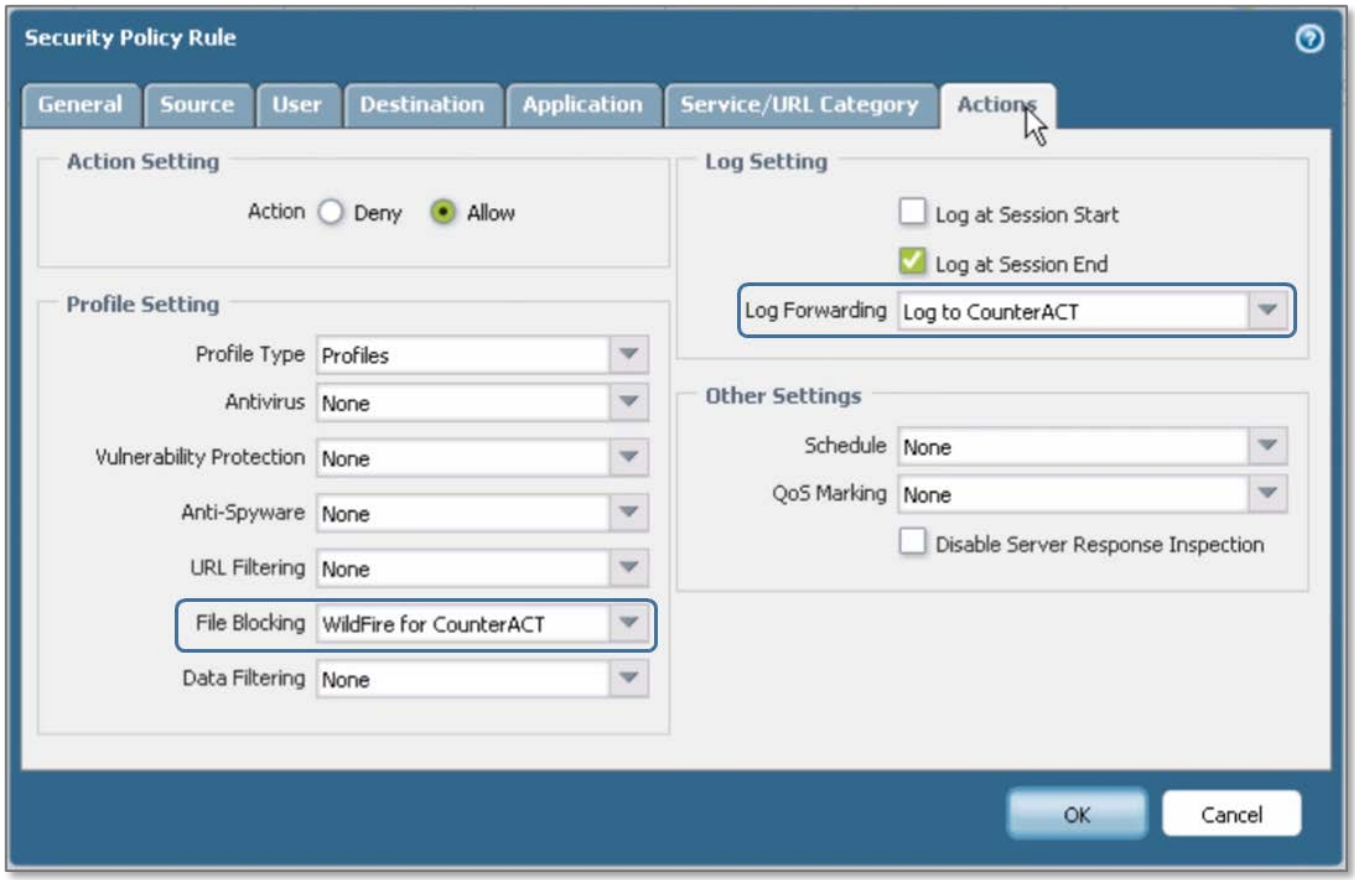
[3] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.

ESG Lab Tested

ESG Lab evaluated ForeScout CounterACT's integration with Palo Alto Networks NGFW to validate the ability of the joint solution to segment resources on a need-to-know basis, assign access to resources on the move, and enable Palo Alto Networks to create granular access policies based on user and device context. Furthermore, the integration with Palo Alto Networks WildFire threat analysis service was examined in the context of threat analysis and mitigation.

ESG Lab configured the integration between ForeScout CounterACT and Palo Alto Networks NGFW and WildFire service in just a few steps. First, ESG Lab configured the ForeScout Extended Module for Palo Alto Networks NGFW and the ForeScout Extended Module for Palo Alto Networks WildFire. Next, the Palo Alto Networks NGFW was configured to communicate with all CounterACT devices on the network as syslog servers. Finally, we configured a Security Policy for outbound Internet access and set the NGFW to forward logs to CounterACT and to block files using WildFire for CounterACT, as seen in Figure 3. The whole process took less than a minute. We used the built-in CounterACT policies for WildFire.

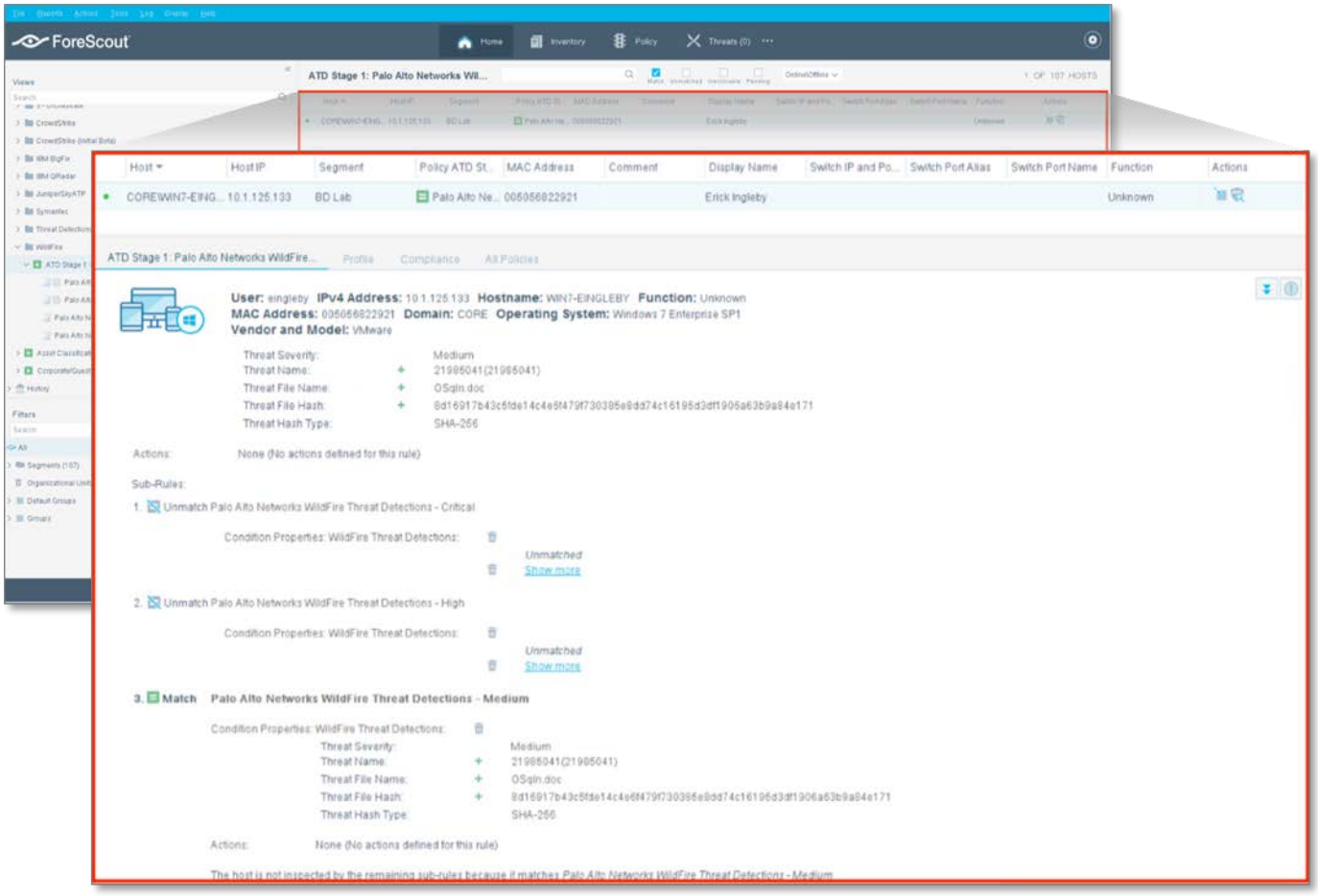
Figure 3. Configuring Palo Alto Networks Security Policy for the WildFire Extended Module



At this point, we were ready to test the integration. We logged in to a Windows machine on the network and downloaded a pre-staged malicious file from a server on the Internet. WildFire analyzed the file and sent the basic scan results to the NGFW, which the NGFW sent to CounterACT via syslog. At this point, CounterACT reached out to WildFire, and retrieved detailed information on this IOC.

Next, ESG Lab looked at the ForeScout Home tab, where we saw that CounterACT had identified the compromised endpoint, as shown in Figure 4. The endpoint was found to have a critical severity threat. CounterACT can take a wide variety of policy-based host or network actions, including modest actions like warning users via HTTP pop-up notifications and warning administrators via email, or more stringent actions such as deleting the file, killing the running process, and isolating the endpoint on the network.

Figure 4. ForeScout CounterACT Threat Detection with WildFire



Why This Matters

With the rapidly evolving threat landscape growing more difficult to manage, it's no wonder that cybersecurity initiatives represented the IT priority most often cited by ESG research respondents in 2017.[4] Palo Alto Networks NGFWs provide network access control based on user, device, application, and traffic classification, leveraging user and device context from a variety of sources to enforce granular access policies with precise and flexible control over resources. Palo Alto Networks WildFire offers a cloud-based, community-driven approach for detecting unknown threats that frequently bypass traditional security defenses.

The ability to detect and respond to multi-vectored, stealthy, and targeted advanced threats is a challenge for organizations today. With a significant number of unmanaged endpoints on organizations' networks, whether BYOD, corporate assets with nonfunctional agents, or IoT devices, a solution that can enable organizations to automatically detect, respond to, and mitigate threats is needed.

ESG Lab has validated that ForeScout CounterACT detects and profiles endpoints as they connect to the network—whether managed or unmanaged—and deeply integrates with Palo Alto Networks NGFWs and WildFire cloud-delivered, advanced threat analysis security service to continuously monitor and remediate endpoint vulnerabilities and security gaps and provide automated incident response to known and unknown attacks and security breaches.

[4] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, March 2017.

The Bigger Truth

The unprecedented diversity of users, devices, and applications on networks—where employees, contractors, guests, and partners often use personal devices to connect to network resources—challenges businesses to efficiently provide them all with appropriate network access.

Palo Alto Networks next-generation firewalls provide network control based on user, device, application, and traffic classification. User and device context from a variety of sources is leveraged to enforce granular access policies with precise, flexible control. Palo Alto Networks WildFire is a cloud-based, community-driven service for detection of threats that frequently bypass traditional security defenses. WildFire leverages a malware analysis environment in which new and unknown malware and exploits can be identified automatically and conclusively using multiple, independent techniques to resist evasion. WildFire then generates automatic protections and distributes them for enforcement.

Palo Alto Networks NGFWs provide network control based on user, device, application, and traffic classification. User and device context from a variety of sources is leveraged to enforce granular access policies with precise, flexible control. Palo Alto Networks WildFire is a cloud-based, community-driven security service for detection of advanced threats that frequently bypass traditional security defenses. WildFire leverages a malware analysis environment in which new and unknown malware and exploits can be identified automatically and conclusively using multiple, independent, and custom-built techniques to resist the most advanced evasion techniques. WildFire then generates automatic protections every five minutes and distributes them for enforcement.

ESG Lab was quite impressed with ForeScout CounterACT's ability to empower organizations using Palo Alto Networks NGFW and WildFire service to efficiently provide visibility and control of endpoints on the network, enabling dynamic segmentation of network resources and providing access regardless of location. In addition, organizations can enforce identity and context-aware security policies to reduce their attack surface, limit data breaches, and detect and remediate advanced threats.

ForeScout CounterACT demonstrated that it can provide visibility, intelligence, and policy-based mitigation of security issues by providing real-time insight into the vulnerabilities and security gaps on managed and unmanaged devices while coordinating security controls and automating responses to rapidly contain threats and breaches. If your organization is currently using or considering Palo Alto Networks for network security, it would be a smart move to look at how ForeScout CounterACT can work with Palo Alto Networks solutions to improve security and reduce the attack surface with automated detection and remediation.